ecora

Ecora Enterprise Auditor for Lotus® Domino Servers

Evaluation Guide

Table of Contents

Getting Started 3
Collecting Data 3
Ecora Reports 5
Generate a Fact-Finding Report 6
Generate a Documentation Report 7
Generate a Baseline Report 8
Schedule an Alert for a Consolidated Change Log Report 9
Check Your Compliance with a Policy 10
To create a group: 10
To create a policy: 11
To calculate compliance to a policy: 12
Congratulations! 12
Customer Support 12

Introduction

This evaluation guide provides an overview of the features of Ecora Enterprise Auditor and a cursory walk-through of the software functionality, aiming to consume less than an hour of your time. It attempts only to show the highlights of how the software might help you with compliance audits, security analysis, disaster recovery, and other projects; not to detail all of the software's capabilities. The user manual (online help system and printable PDF) provides a much more thorough explanation of each software feature and function.

Enterprise Solution

Ecora offers solutions for:

- Active Directory systems
- Cisco routers and L3 switches
- Citrix MetaFrame servers
- Lotus Domino servers
- Microsoft Exchange servers
- Microsoft Internet Information Services
- Microsoft SQL servers
- Microsoft Windows servers
- Microsoft Windows workstations
- Novell NetWare servers & NDS
- Oracle databases
- Unix systems (HP-UX, AIX, Linux, Solaris)

Install the Software

This Evaluation Guide assumes that you have successfully downloaded, installed, and configured Ecora Enterprise Auditor.

If you have not, please refer to the **Start-up Guide**, located on Ecora's website at: (http://www.ecora.com/ecora/um/startup_guide-auditor4.0.pdf).

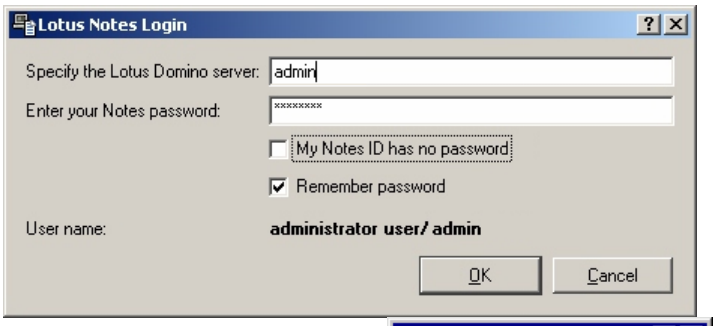
Getting Started

This section will locate systems in your environment, collect configuration information about the systems you select, and set up regular collection. Since reports can always be run against existing data, it makes sense to get into the habit of regular data collection, which Ecora allows you to automate completely with scheduling.

There are two basic aspects of scheduling: selecting systems and scheduling the time, date, and frequency. Selection sets contain a list of systems and scheduling assigns a time, date, and frequency to the selection set.

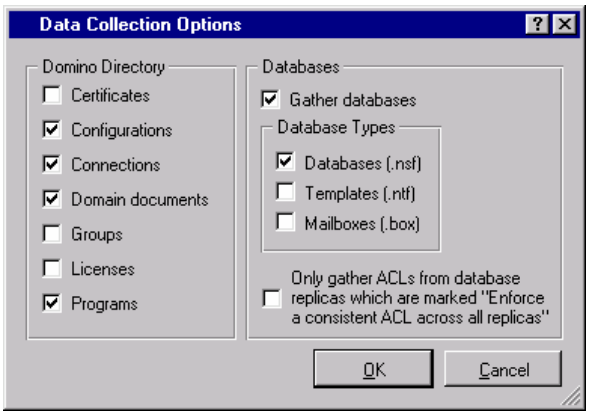
Collecting Data

1. Click on the **Collect** button.
2. Select the **Data Collection**, select **Full Report**, and click **Next >**.
3. If prompted, enter the Preparer settings (your name, email, and organization), enable the option to **Always use these settings**, and click **OK**.
4. Enter the name of a Domino server.

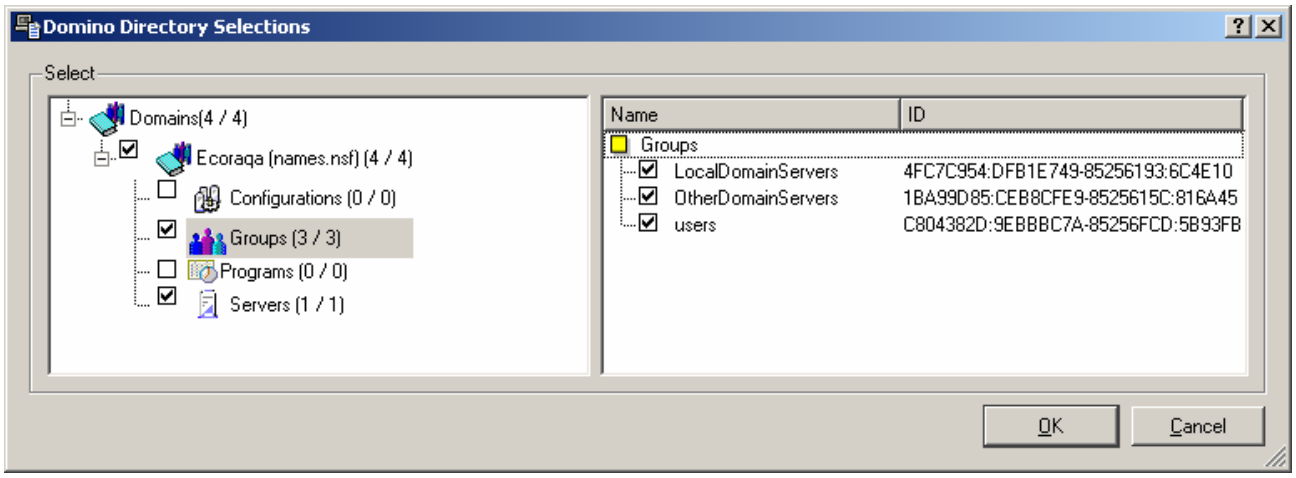


Tip: Document one of your hub servers for the most data.

5. Enter your Lotus Notes CLIENT password (or select the **My Notes ID has no password** option).
6. Click **OK**.
7. Select domain(s) you're interested in collecting (and reporting).
8. Select the types of data you're interested in collecting (and reporting).



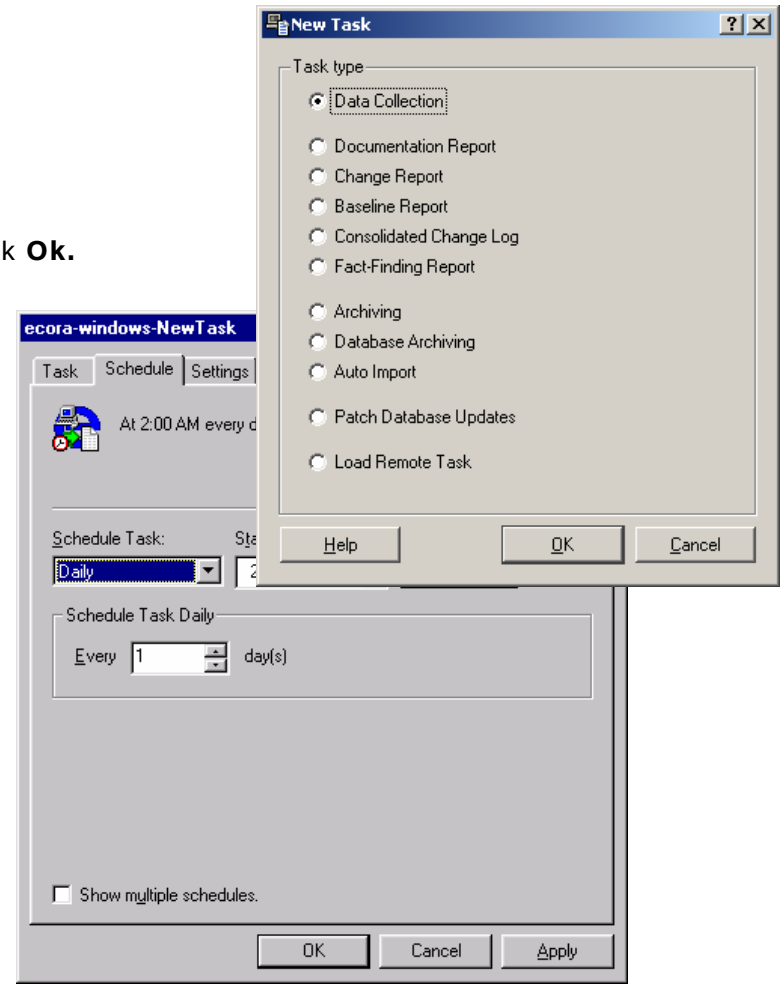
9. Click **OK**.
10. If prompted, navigate the tree to select the specific objects you'd like reported.
11. Click the **OK** button to begin collection.



12. Click **Yes** when prompted to save this selection to a file for scheduling.
13. Enter a name, such as “Evaluation” that you’ll remember and click **OK**.
14. Once collection has completed, click **Finish**.

Scheduling Collection

1. Go to **Scheduled Tasks** tab.
2. Click **New task**….
3. Choose **Data Collection** and click **Ok.**
4. Name the Task “Nightly” and click **Ok.**
5. Accept the default data file name and choose “Evaluation” from the drop-down list (or choose interactively and repeat the prior section).
6. Click **OK**.
7. On the **Task** tab, click the **Set Passwords** button.
8. Enter a valid password twice and click **OK**.
9. Click on the **Schedule** tab, click **New**.
10. Set the task to run **Daily** with start time **2am**.
11. Click **Apply**, then **OK**.



Ecora Reports

Once you begin collecting data, it is available for reporting, querying, and archiving. Ecora Auditor offers more reporting options than ever, allowing you to answer virtually any question you might have about your infrastructure. Ecora's range of reports provides you an assortment of ways to extract valuable data in the best format for your needs.

Documentation Reports - These full-text reports preserve the strengths of past Ecora versions for compliance audits, detail disaster recovery plans, security assessments, migration plans, troubleshooting, and preserving IT knowledge and decisions.

Fact-Finding Reports - These reports more closely resemble database queries for several reasons: they pull data from the cross-platform configuration database and they allow use of operators, so you can search for values greater than, less than, or unlike a threshold value you set. These reports are very surgical in their precision - you can pull precisely the data you need, but they also offer a wealth of data through hundreds of built-in reports created by experts.

Change Reports - Change Reports offer the ability to quickly see "before" and "after" snapshots of systems in your environment. Great for pinpointing a setting change that indicates a security breach or is the cause of your troubleshooting problem. These concise reports find any planned, unplanned, or even unauthorized, changes!

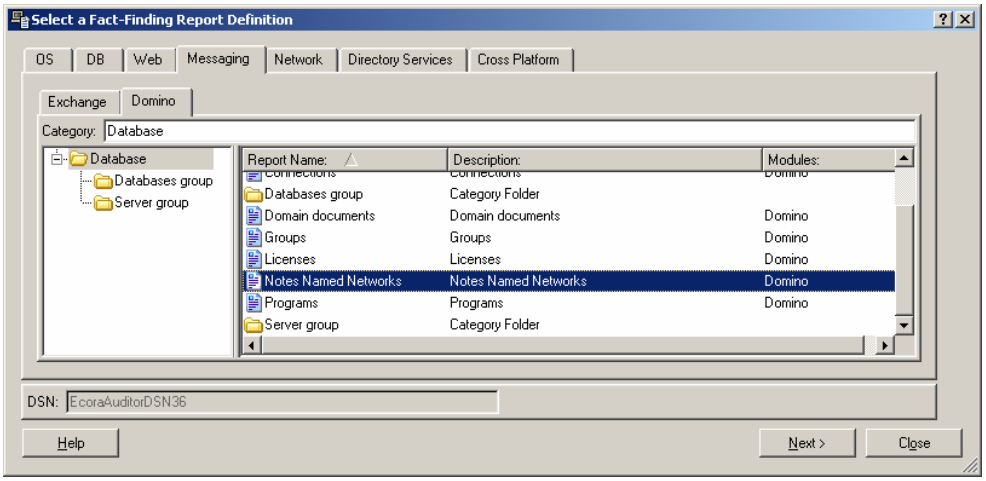
Consolidated Change Logs - These reports add a valuable dimension to change tracking. In addition to "before" and "after" data, these (CCL) reports can show EVERY change that occurred in a given time period - across multiple platforms. These reports answer the call for change histories for auditors and intensive security monitoring systems.

Baseline Reports - Everyone understands the value of keeping consistency in configurations... keeping machines to current patch levels for security, maintaining QA or policy standards, compatibility and maintenance of core technology, passing compliance audits, performance, and much more. Baseline Reports are the best way to quickly locate differences among systems in your environment. Choose any machine as a standard and one report shows exactly how any others you select deviate from that machine's configuration setup.

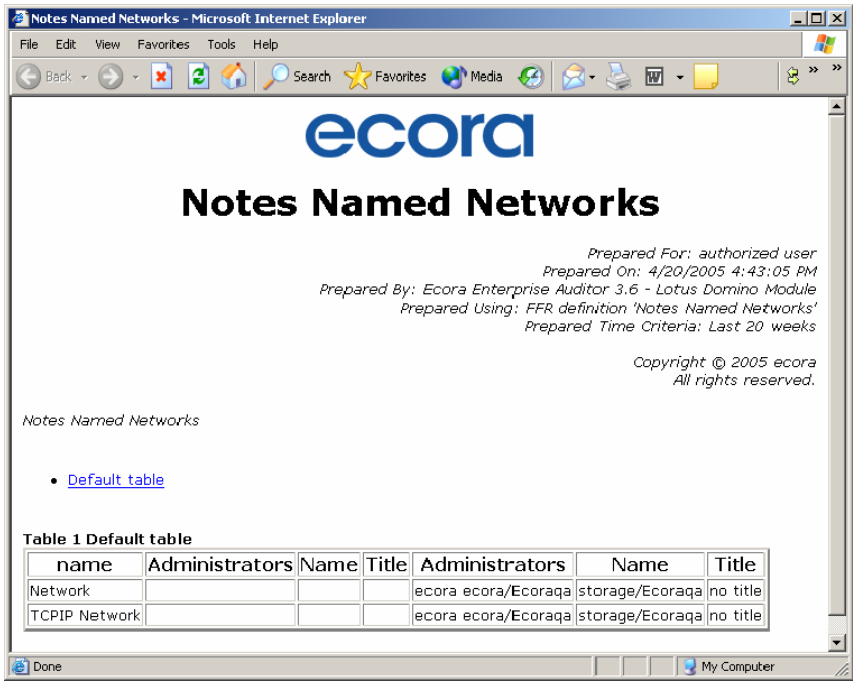
Generate a Fact-Finding Report

Lotus Domino experts created a collection of reports that solve common problems or target IT projects, then included these reports in the software. These “report definitions” act like templates, creating the structure of the report, which is filled in with actual content from your environment. These report definitions can be used or customized to your specification.

1. Click on the **Fact-Finding** button.
2. Click on the **Database** node plus sign to expand the tree.
3. Take a minute to explore the available reports that have been provided. Any can be generated, scheduled, or customized.
4. Select a report that interests you.
5. Click on the **Next >** button to proceed.



6. If you wish to see how the report is constructed, select the table and click the **Edit** button. Click **Close** once you’ve reviewed the structure.
7. Click **Generate >**.
8. Accept the timestamp name and click **OK**.
9. When the report finishes, click **View** to see the finished report as an HTML page in a browser.
10. Scroll down to see how each is configured.



Tip: Remember - any report can be scheduled to occur daily, weekly, or once after hours.

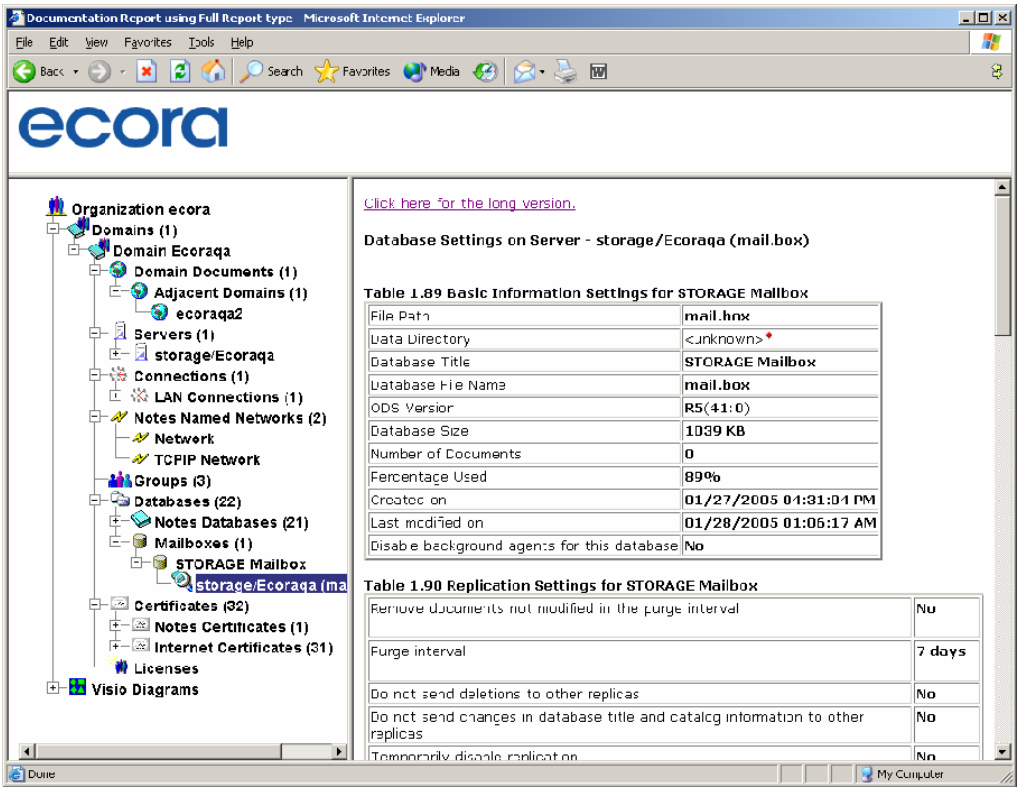
Generate a Documentation Report

1. Click on the **Document** button.
2. Verify that the **Documentation Report** and **Full Report** type are selected.
3. Click **Next >**.
4. Choose to **Use Existing Data** and click **Next >**.
5. Select the data set you just collected and click **Next >**.
6. After the report has been generated, click **Finish** to View Report Now.

Browse the Report

A browser opens displaying the HTML report with a directory tree in the left frame and the content in the right frame. The directory tree is both an overview and a navigational device, allowing you to locate and open specific sections of the report.

1. Click on the top node plus sign to expand the tree to display the available domains.
2. Click on one of the database nodes.
3. Review the report. Are any of the settings concerning?
4. Browse through the sections of the report to get a feel for the scope of the information and how features such as Visio diagrams could save time in your IT projects.

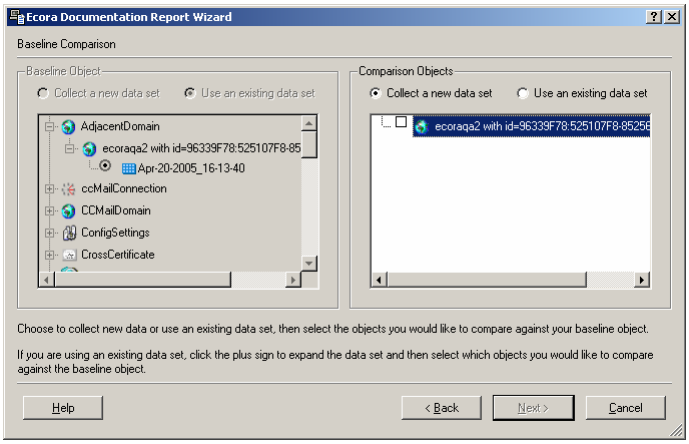


5. Click on the link labeled **Click here for the long version** to toggle between the detailed long form or the "just the facts" short form for as much detail as you desire.
6. Particularly in the long version, look for the tips, notes, alerts, and references provided by Microsoft Windows experts. These icons call your attention to important information, such as security risks or relevant articles / resources.

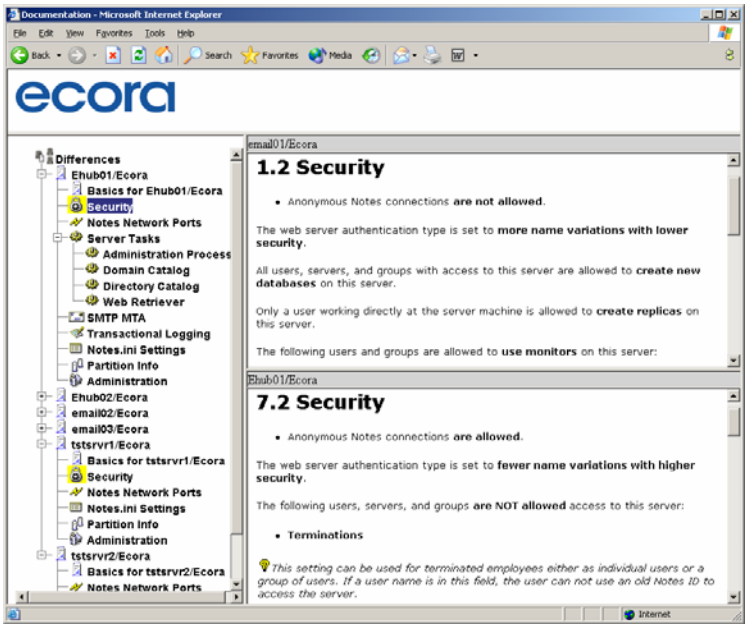
Generate a Baseline Report

Baseline reports identify deviations from any selected standard, invaluable in locating non-standard configurations, insecure settings, or compromising access rights.

1. Click on the **Baseline** button.
2. Verify that **Baseline Comparison Report** is selected and that Report Type is **Full Report**.
3. Click the **Next >** button.
4. Choose to **Use an existing data set** in the Baseline Object area.
5. Locate and choose a Baseline Object in the left pane. For this evaluation, locate and select your saved data set and select one system to be the standard.
6. Click **Next>**.
7. Choose to **Collect a new data set** in the Choose Comparison Objects area.
8. Locate and select the Comparison Object(s) in the right pane. Choose the remaining systems allowed by your trial license.


Ecora Documentation Report Wizard
Baseline Comparison
Baseline Object
Collect a new data set
Use an existing data set
AdjacentDomain
ecoraqa2 with id=96339F78:525107F8-85
Apr-20-2005_16-13-40
ccMailConnection
CCMailDomain
ConfigSettings
CrossCertificate
Comparison Objects
Collect a new data set
Use an existing data set
ecoraqa2 with id=96339F78:525107F8-85256
Choose to collect new data or use an existing data set, then select the objects you would like to compare against your baseline object.
If you are using an existing data set, click the plus sign to expand the data set and then select which objects you would like to compare against the baseline object.
Help
< Back
Next >
Cancel

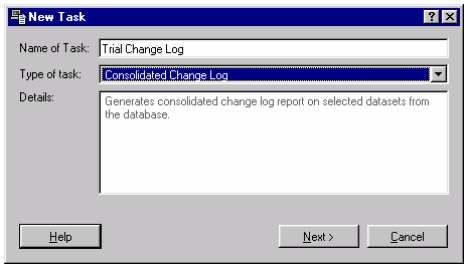
9. Click **Next>**.
10. If prompted to verify the Selection Editor, click **OK** to accept the default settings. You can use the tree to locate and select data/objects you want to compare against your baseline or “Gold Standard” system.
11. Click **OK**.
12. After the report has been generated, click **Finish** to View Report Now.
13. Browse the split-screen HTML baseline report, using the directory tree to compare each system to your standard. The top section of the right frame contains the reference server (your "gold standard") and the bottom section contains the selected target server's differences when compared against the standard system.


Documentation - Microsoft Internet Explorer
ecora
Differences
Ehub01/Ecora
Basics for Ehub01/Ecora
Security
Notes Network Ports
Server Tasks
Administration Process
Domain Catalog
Directory Catalog
Web Retriever
SMTP MTA
Transactional Logging
Notes.ini Settings
Partition Info
Administration
Ehub02/Ecora
email02/Ecora
email03/Ecora
tstsrvr1/Ecora
Basics for tstsrvr1/Ecora
Security
Notes Network Ports
Notes.ini Settings
Partition Info
Administration
tstsrvr2/Ecora
Basics for tstsrvr2/Ecora
Notes Network Ports
email01/Ecora
1.2 Security
Anonymous Notes connections are not allowed.
The web server authentication type is set to more name variations with lower security.
All users, servers, and groups with access to this server are allowed to create new databases on this server.
Only a user working directly at the server machine is allowed to create replicas on this server.
The following users and groups are allowed to use monitors on this server:
Ehub01/Ecora
7.2 Security
Anonymous Notes connections are allowed.
The web server authentication type is set to fewer name variations with higher security.
The following users, servers, and groups are NOT allowed access to this server:
Terminations
This setting can be used for terminated employees either as individual users or a group of users. If a user name is in this field, the user can not use an old Notes ID to access the server.

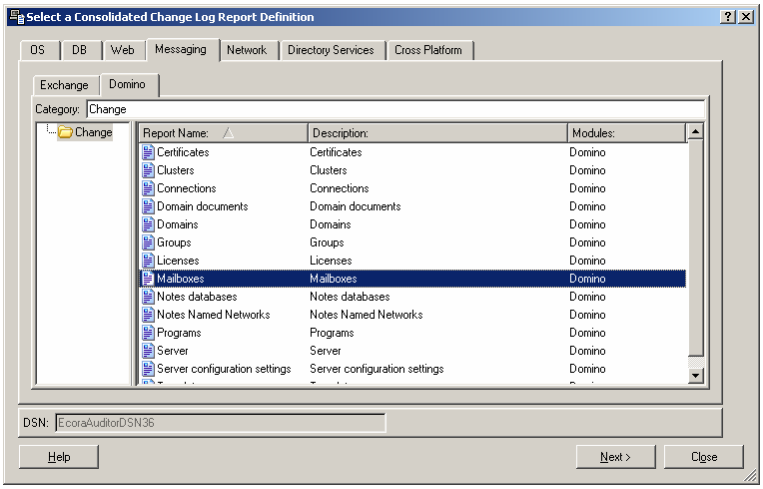
14. In particular, check the security differences. Are all your systems secured?
15. Browse the other sections to see where your systems differ.
16. Close the report when you’re done.

Schedule an Alert for a Consolidated Change Log Report

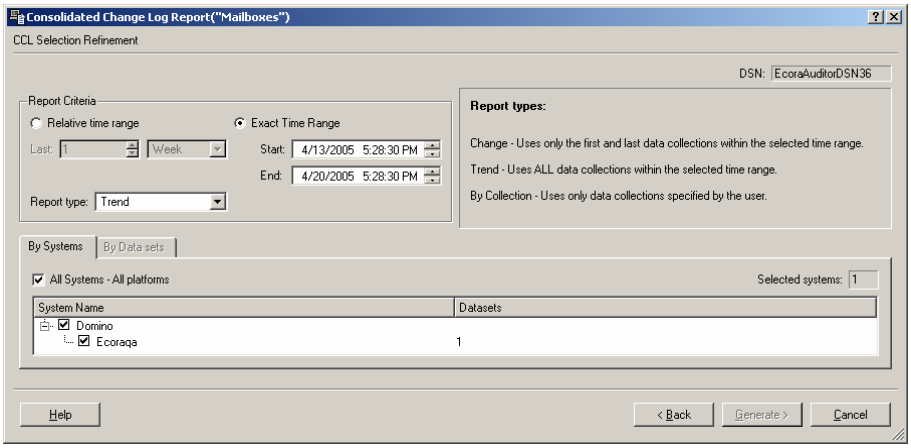
This section is strictly optional, but introduces you to the tip of the iceberg in automating scheduled reports and using Ecora's proactive alerting capabilities. If you complete this section, you will be rewarded with a Consolidated Change Log emailed to you at the end of the evaluation period.



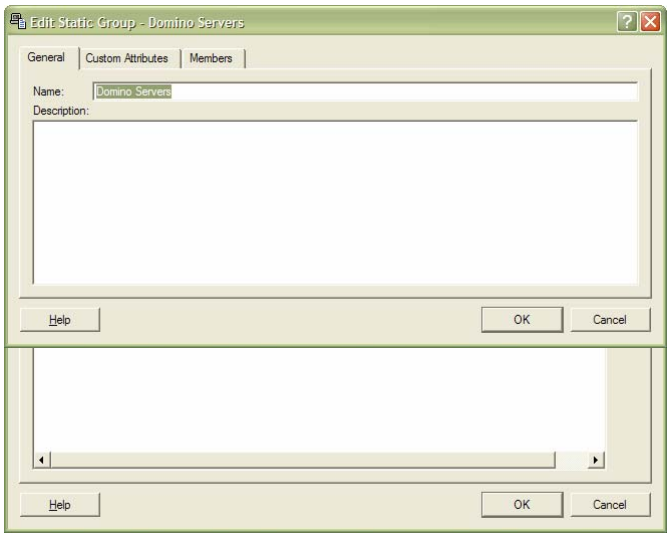
1. Click on the **Scheduled Tasks** tab.
2. Click **New Task…**.
3. Choose **Consolidated Change Log** and click **OK**.
4. Enter a task name, such as "Trial Change Log" and click **OK**.
5. Select the **Mailboxes** report and click **Next >**.
6. Accept all the settings and click **Next** >.
7. Change to **Exact Time Range** and set the End date to ten (10) days from today.
8. Change the Report Type to **Trend** in the drop-down list.
9. Click in the checkbox for **All Systems** and click **Next >**.
10. Accept the date/time default naming convention and click **OK**.



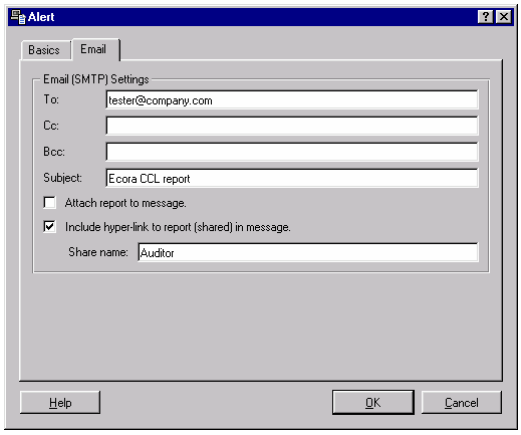
11. On the **Task** tab, click on the **Set Passwords** button.
12. Enter the password twice and click **OK**.
13. Click on the **Schedule** tab, click on the **New** button.
14. From the drop-down lists, set the task for **Once** at **6:00 AM**.
15. In the Run on area, choose the date ten (10) days from today.
16. Click **Apply**, then **OK**.



17. Choose **Edit… Alerts and Triggers…** from the menu.
18. Click **New…**.
19. Select an **Email Alert** and click **OK**.
20. On the Basics tab, enter a Name (such as "CCL test alert") and Description for the alert.
21. On the Email tab, enter your email address in the To: field.
22. Click in the **Include hyper-link to report** option and click **OK**.



23. Click on the **Triggers** tab (if the box closed, choose **Edit… Alerts and Triggers…**).
24. Click **New…**.
25. On the Basics tab, enter a Name and Description.
26. On the Conditions tab, click in the Domino checkbox and select **Consolidated Change Log Report** from the drop-down list.
27. Choose **Success** from the Condition drop-down list.
28. On the Alerts tab, click in the checkbox next to the Alert you created (suggested: CCL test alert) and click **Close**.
29. Look forward to getting an email in a week or so!



Check Your Compliance with a Policy

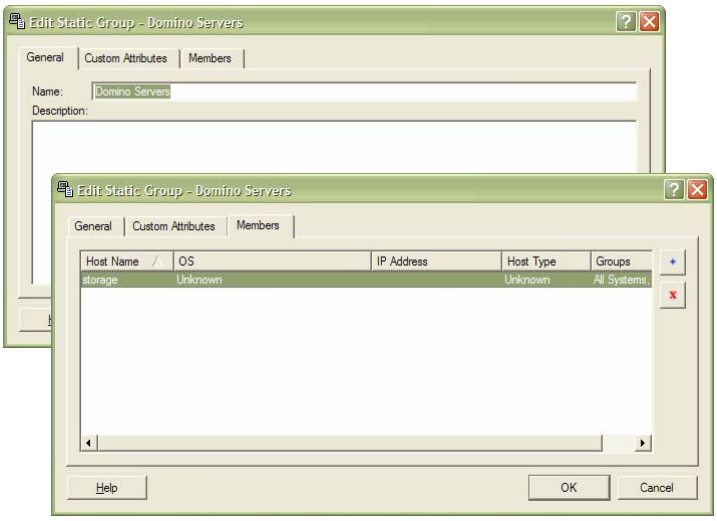
Auditor now includes the ability to define policies for security, federally regulated standards, corporate standards, as well as an interface to graphically display compliance levels for a quick and concise visual of compliance status. Ecora provides a series of policies with the software that you can use to check your environment for compliance or customize to suit your needs.

Note: This section presumes that Policy Compliance Dashboard has been installed and configured according to the **Startup Guide**, located on Ecora's website at: (http://www.ecora.com/ecora/um/startup_guide-auditor4.0.pdf).

To create a group:

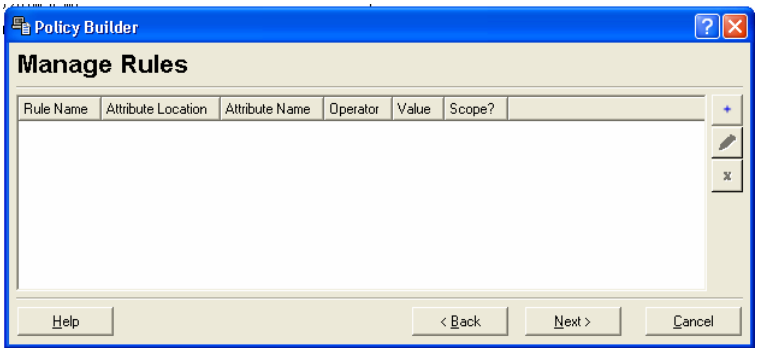
1. Select the **Policies** tab on the main screen of Auditor.
2. Expand Groups to show the All Systems Group.
3. Right-click on the All Systems Group and select **New Static Group**.

4. Enter a name for the group in the Name field – such as Domino Servers.
5. Select the **Members** Tab.
6. Click on the **Add** button to add systems to the group.
7. Select a Domino server from the list of available systems and click **OK**.

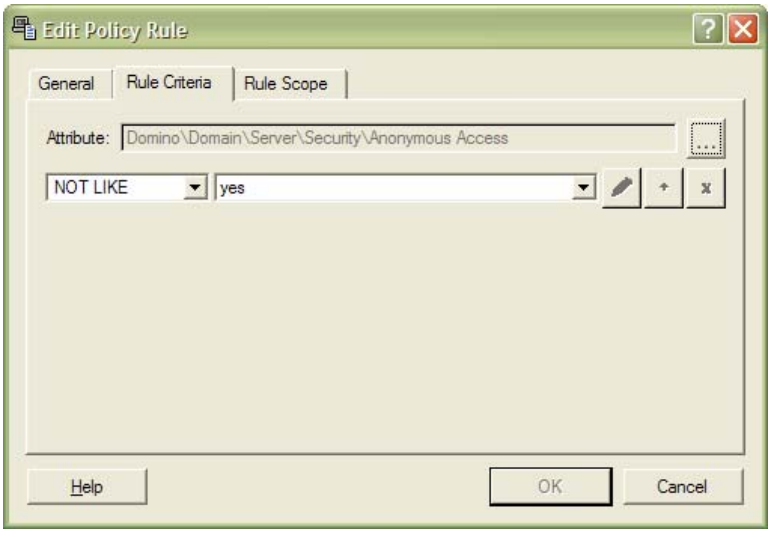


To create a policy:

8. Right-click on **Policies** and select **New Policy**.
9. Uncheck **Import system configuration as policy** and click **Next**.
10. The Manage Rules dialog that appears; click the **Add** button to the right.



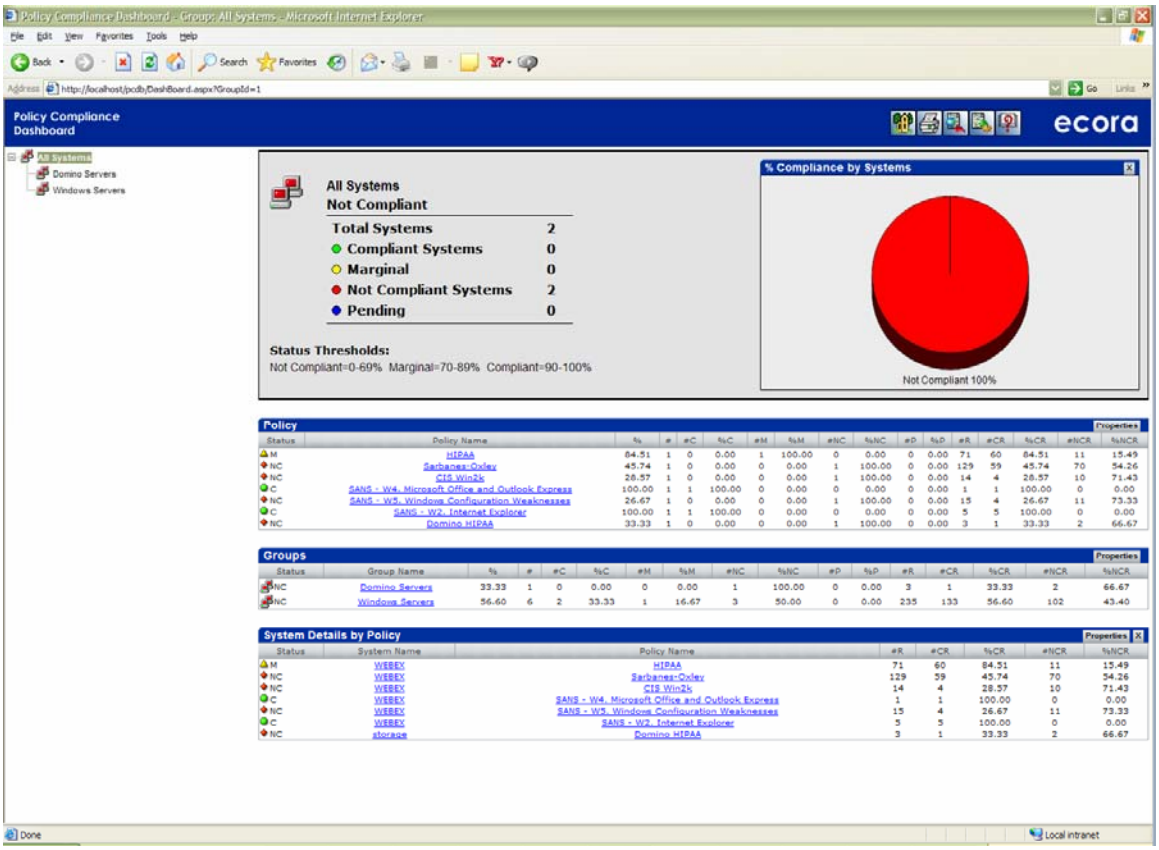
11. The Select a Rule Attribute window appears. Click on the **Messaging** tab.
12. Expand the tree, locate, and select the **Anonymous Access** attribute for this policy.
13. Click **Next**.
14. Use the drop-down list to select the NOT LIKE operator.
15. Enter YES for a value.
16. Click **OK**.
17. Click **Finish** and the Manage Rule Scope window appears. Make no changes.
18. Click **Next**.
19. You can change the Rule name and add a Rule Description.
20. Click **Finish** to complete the policy.
21. Right-click on the new policy and select **Apply Policy**.



22. Select the group created above – Domino Servers – and select **OK**.

To calculate compliance to a policy:

1. Run **Policy Compliance Dashboard** from the icon on the desktop.
2. Click on the **Domino Servers** group in the tree on the left.
3. Review the pie chart in the upper right to see the percentage of your systems that are compliant (green), non-compliant (red), marginal (yellow), or pending (blue).



4. Click on a system in the **System Details by Policy** block to see how the system compares to the rules that define this policy.
5. Drill down to the rule level to see the settings on a specific system to see why it does not comply with the new policy.
6. Close the dashboard browser.

Congratulations!

You have completed the Ecora Enterprise Auditor evaluation. There are many more reports, alerts, creative queries, and practical applications for the software, but we hope that this evaluation guide helped you get through the highlights efficiently. Thanks for your time.

Customer Support

Ecora technical support representatives are available to answer your questions at 1.877.923.2672 or email support@ecora.com.